블록체인 기법을 사용하는 전자화폐 사용자의 프라이버시 보호에 대한 연구

강용혁*

*극동대학교

A Study of Privacy Protection for Users of Electronic Money Using Blockchain Technology

Yong-Hyeog Kang*

*Far East University

E-mail : yhkang@kdu.ac.kr

요 약

전자화폐를 구현하는 블록체인 기술은 분산화된 컴퓨팅을 사용하며 모든 거래가 모두에게 공개되어 있다. 이러한 기술은 사용자 대신 주소를 사용하여 거래에 수행하여 익명성을 보장하는 것처럼 보이지만 거래 그래프를 기반으로 비순환 방향 그래프를 이용하여 공개된 주소를 추적함으로써 프라이버시 문제가 발생하게 된다. 본 논문에서는 블록체인 기술 내에서 발생하는 프라이버스를 보호하기 위하여 그래프 상의 관련성을 찾기 어렵게 하는 중앙 집중적으로 처리하는 다양한 기법들을 분석한다. 또한, 프라이버시를 강화하기 위하여 분산화된 방법으로 익명화하는 기법들도 분석한다. 영지식 증명 기법을 이용하면 완전 분산 익명성을 보장하지만 더 많은 연산과 저장 공간이 필요하게 되며, 이를 효율적으로 하기 위한 여러 가지 기법들도 제안되었다. 본 논문에서는 기존 프라이버시 보호 기법들을 블록체인 기술에 융합하여 블록체인 기술의 프라이버시 보호를 위한 기법을 제안한다.

ABSTRACT

The blockchain technology that implements electronic money uses decentralized computing and all transactions in a blockchain are open to everyone. This technique seems to guarantee anonymity by performing the transaction on the address instead of the user, but by using direction acyclic graph based on the transaction graph, the privacy problem is caused by tracking the addresses. In this paper, we analyze various techniques for centralized processing which makes it difficult to find the relevance on the graph in order to protect the privacy in the block chain technology. We also analyze the techniques of anonymizing in a distributed way to enhance privacy. Using the zero knowledge proof scheme guarantees full distributed anonymity but requires more computation and storage space, and various techniques to make this efficient are proposed. In this paper, we propose a privacy protection scheme of blockchain technology to integrate existing privacy protection techniques into a blockchain technology and perform it more efficiently with a centralized or decentralized technique.

키워드

블록체인 기술, 익명성, 프라이버시, 영지식 증명

Ⅰ. 서 론

블록체인 기술을 사용하는 비트코인(Bitcoin)과 같은 화폐 시스템은 중앙집중식이 아닌 암호화된 화폐(cryptocurrency) 시스템이다. 이러한 시스템의 특징은 모든 트랜잭션의 완전한 목록이 공개되고 연결되어 있다는 것이다[1].

암호화된 화폐는 익명으로 인식되었지만 블록체인으로 인해 사용자의 트랜잭션은 연결되어 사용자의 익명성이 노출될 수 있다[2]. 본 논문에서는 블록체인 기술을 이용하여 발생하는 프라이버시를 보호에 대한 연구를 수행한다.

Ⅱ. 관련 연구

트랜잭션 그래프는 비트코인 트랜잭션이 정점(vertex)이 되고 트랜잭션의 입력과 이와 연관된 트랜잭션의 출력을 연결하는 선분(edge)으로 구성된다. 이러한 트랜잭션 그래프는 사이클이 없는 DAG (Directed Acyclic Graph)이 된다[3]. 트랜잭션 그래프의 분석에서 동일한 트랜잭션 안에 있는 모든 입력은 단일 사용자로 속한다고 가정할 수 있다. 클로저(closure) 연산 수행 시에 서로 다른 두 개의 주소를 서명하는 사용자는 두 개의 주소에 대한 개인키를 갖고 있으므로 동일한 사용자라고 가정하는 것이다. 재사용 주소도 분석을 용이하게 하며 주소의 변경도 글로저 연산에 포함된다. 클로저 연산을 적용한 결과가 사용자 그래프이다. 정점은 사용자를 나타내며, 선분은 트랜잭션을 나타낸다.

사용자 그래프에 추가적으로 사용자들에 대한 정보를 얻기 위한 다양한 기법들이 적용될 수 있다[3]. 네트워크 이외의 다른 정보들을 이용하여 분석하는 방법이 있으며, IP 트래픽을 분석하는 방법, 네트워크 위상 분석, 클러스터 분석, 흐름과 시간 분석 및 다른 소셜 네트워크의 그래프의 동형 분석 등이 있다. 사용자 그래프 외에 다른 정보는 사용자의 익명성을 무효화시킬 수 있다.

Ⅲ. 블록체인을 위한 프라이버시 보호 기법

세탁물 서비스(laundry service) 또는 혼합 서비스(mixing service)는 사용자에게 자금을 중앙 풀(pool)에 전달하고 나중에 다른 주소로 자금을 가져오는 서비스이다. 서비스 제공자만이 입력과 출력에 대한 연관을 알 수 있어서 프라이버시를 강화할 수 있지만 시빌(Sybil) 공격에 취약하며 풀을 사용하기에 완전한 익명성(full anonymity)을 제공하지 못한다. 그린 리스팅(greenlisting) 또는 주소 확인(validation) 기법은 비공개된 데이터베이스를 이용하여 주소를 등록하게 하여 추적을 어렵게 기법이다.

비집중화 방식으로 익명성을 보장하는 기법들도 제안되었다. CoinJoin 기법은 여러 사용자가 혼합하여 다중 입력과 출력을 갖는 트랜잭션을 만드는 기법이다. Meet-up 서버를 이용하여 참여자들도 자신의 것을 제외하고는 입력과 출력의 매칭을 알지 못한다. CoinSwap 기법은 서드파티가 트랜잭션에 참여하여 지급자 주소와 수신자 주소를 추적하지 못하게 하며 중간자의 가로채기를 방지하기 위해 hashlock 기법을 사용한다. Diffie-Hellman 키교환 기법을 사용하는 스텔스(stealth) 주소 기법도 제안되었다. 이 기법은 공격자가 최종 주소를 공개된 시드(seed)와 연관시킬 수 없다.

본 논문에서 제안하는 기법은 다음과 같다. 전자 화폐는 익명성을 보장해야 하지만, 전자화폐가 완전한 익명성을 제공하는 경우에는 범죄에 악용될 여지가 있다. 전자화폐를 합법적인 이유로 추적이 필요할 때는 추적이 가능해야 한다. 하지만 최대한의 프라이버시를 제공해야 한다. 대표적인 프라이버시 기법은 k-anonymity 기법이다[4]. 그림 1은 제안 기법의 주소 변환 기법이다.

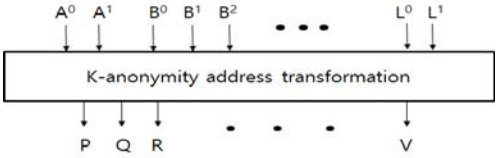

그림 1. 제안 기법의 주소 변환 기법

제안기법은 여러 사용자의 주소를 동시에 변환하여 사용자와의 관계에 k-anonymity를 적용한다. 즉, k개의 주소가 공개되어도 사용자를 구분할 수 없는 기법이다. 또한, 이러한 주소는 인증기관과 같은 제 3자의 신뢰기관에 비밀리에 보관하여 합법적으로 추적이 필요할 경우 추적이 가능하도록 한다.

Ⅳ. 결론 및 향후 연구과제

본 논문에서는 블록체인을 사용하는 전자화폐가 사용자의 프라이버시를 보장하기 위해 여러 가지 기법들이 제안된 것을 설명하였다. 또한, k-anonymity를 이용하여 프라이버시를 보장하는 기법을 간략히 제안하였다. 향후 연구과제로는 현재 사용되고 있는 암호화 프리미티브를 이용하여 제안 기법을 상세화하고 프로토콜을 개발하여 검증하고 구현하여 테스트하는 것이다.

참고문헌

[1] D. D. F. Maesa, et al, Uncovering the Bitcoin Blockchain: An Analysis of the Full Users Graph, In Data Science and Advanced Analytics (DSAA), 2016 IEEE International Conference on.

[2] E. Heilman, et al, Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions, In Workshop on Bitcoin and Blockchain Research at Financial Crypto, February 2016.

[3] P. Franco, Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley, 2014.